Information Security Managers Group
Thursday, September 30, 2010 Meeting Minutes

MEETING LOGISTICS (all meeting minutes are posted on the ISMG Sharepoint site:
http://ent.sharepoint.mt.gov/groups/ism/default.aspx)

When: Last Thursday of each month 1:00 pm – 2:30 pm
Who: Agency CIO and/or Information Security Manager
Where: Department of Labor and Industry First Floor Conference Room
Corner of Lockey and Sanders
Next Meeting: Tentative – October 29, 2010 1:00 pm

PRESENT

MDT:	Kristi Antosh
DLI:	Judy Kelly
DLI:	Lance Wetzel
DOA:	Kevin Winegardner – Chair
DOA:	Larry Manchester
OPI:	Joan Anderson
FWP:	Barney Benkelman
DNR:	Rick Bush
AGR:	Libbi Lovshin
DOC:	Larry Krause

PURPOSE

The Information Security Managers Group has three primary purposes:

- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

AGENDA ITEMS

- **Welcome and (re)introductions**
  - It was identified that the players already knew each other and introductions were not necessary.

- **Training on NIST Controls – Control Family – Program Management Control PM-3 "Information Security Resources"**
  - Discussion:
    - The control concept was reviewed briefly, main points were:
      - Information Security Programs require a capital planning and investment process that synch's up with the overall EPP/budgeting process of the agency.
      - The CPIC process should have touch points with the SDLC of the agencies business information system and projects generated by the operation of those business systems.

- **Discussion: "Statewide Standard: Identification and Authentication"**
  - Team wants to revise language in draft standard in section around frequency of review. Something to the effect of "As defined in the Information System Authorization package",

or "As determined in the information system security plan", etc… See draft document here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Policy%20Instruments/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPolicy%20Instruments%2fStatewide%20Standards&FolderCTID=&View=%7b6DB407C1%2dDFA4%2d478B%2dA2BD%2d69F9D61CE7EF%7d

- **Action**:
  - Revise draft language and post on ISMG SharePoint site.
    - **Who**: CIO Policy Office and ISMG Chair

- **Status Update: State CIO decision package legacy IT policies:** Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors
  - State CIO has approved the ISMG decision package recommending revising the above legacy IT security policies into a single "Statewide Standard: Access Control", and "Statewide Guideline: Access Control".
    - **Action**:
      - Post draft "Statewide Standard: Access Control", for review on ISMG SharePoint site here in Statewide Standards folder: http://ent.sharepoint.mt.gov/groups/ism/irmp/Policy%20Instruments/Forms/AllItems.aspx?View=%7b6DB407C1%2dDFA4%2d478B%2dA2BD%2d69F9D61CE7EF%7d
        - **Who**: CIO Policy Office and ISMG Chair
      - Review draft "Statewide Standard: Access Control"
        - **Who**: ISMG development Team

- **Discussion: State CIO decision package on legacy IT policies:** Internet and Intranet Security and Internet Filtering.
  - The Team would like to review rescission language that would be used to rescind the legacy policies, if the State CIO approves the decision package recommending rescinding both legacy policies**.** Draft language posted here in Sample Agency Instruments folder: http://ent.sharepoint.mt.gov/groups/ism/irmp/Policy%20Instruments/Forms/AllItems.aspx?View=%7b6DB407C1%2dDFA4%2d478B%2dA2BD%2d69F9D61CE7EF%7d
    - **Action:**
      - Produce rescission language, post for review on ISMG site.
        - **Who**: CIO Policy Office and ISMG Chair
      - Review rescission language for acceptability
        - **Who**: ISMG development Team
  - The Team would also like the opportunity for all Agency Information Security Managers to review ENT-INT-011 "Internet Acceptable Use", to determine if this policy will meet the requirements of those wishing to reference statewide policy for HR purposes of determining internet acceptable use.
    - **Action:**
      - See ENT-INT-011 "Internet Acceptable Use", here: http://itsd.mt.gov/policy/policies/Asset_Usage/assetusagedomain.mcpx
      - Review ENT-INT-011 "Internet Acceptable Use", for acceptability
        - **Who**: ISMG development Team

- **ISMG NIST: In-house** Training 'Applying the NIST Information Risk Management Framework' and 'Managing an Information Security Program' seminars to the state. See complete list of seminars here: http://www.misti.com/default.asp?Page=31&Type=3&Cat=168

- **Action**:
  - Ascertain options and requirements for bringing NIST training from MISTI in-house.
    - **Who**: MDT ISM

OTHER PENDING ACTION ITEMS

- Develop a visual representation of Policy, Standard of Performance, Guideline, and Procedure taxonomy. Post to ISMG Sharepoint site. (Companion Visual to go with spreadsheet "Connect Dots Ext Req to Procedures" here: http://ent.sharepoint.mt.gov/groups/ism/ate/Policy%20Standard%20Guidelines%20Procedures%20Taxonomy/Forms/AllItems.aspx
  - ISMG Chair

- Develop a visual representation of Sample Program Implementation Strategy. Post to ISMG Sharepoint site. (Companion Visual to go with "Sample Program Implementation Strategy" document here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPlanning%2fNear%2dTerm&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d)
  - ISMG Chair

AGENDA ITEMS FOR NEXT MEETING

- **Training** on NIST Controls – Control Family – Program Management Control PM-4– "Plan of Action and Milestones Process"
  - ISMG Chair
- **Action**: Approve Statewide Standard: Access Control" draft document for proceeding to the next step in the Statewide Policy and Standard development procedure: Submission to State CIO, DOA Legal, DOA Director for review.
  - Development Team (ISMG)
- **Action**: Approve "Statewide Standard: IS Identification and Authentication" draft document for proceeding to the next step in the Statewide Policy and Standard development procedure: Submission to State CIO, DOA Legal, DOA Director for review.
  - Development Team (ISMG)
- **Action**: Approve rescission language for State CIO regarding the legacy IT security policies Internet and Intranet Security and Internet Filtering
  - Development Team (ISMG)
- **Discuss** and Determine recommendation on next legacy IT policies under review*: To be determined
  - Development Team (ISMG)
- **Report** out on In-House NIST Training opportunity with MISTI
  - MDT ISM